Math 615: Lecture of January 5, 2007

This course will deal with several topics in the theory of commutative Noetherian rings, including the following:

(1) The theory of Gröbner bases and applications: a lot more about this momentarily.

(2) The structure theory of complete local rings. One strategy in studying problems over Noetherian rings is to reduce first to the local case, and then to the complete local case. The structure theory of complete local rings can then be applied. There are even deep theorems that permit one to pass from the case of a complete local ring to a finitely generated algebra over a field or complete discrete valuation ring. Other techniques can be used to pass from a problem in such an algebra over a field of characteristic 0 to a corresponding problem over a field, even a finite field, of positive prime characteristic p.

(3) What can one do when a ring is not Cohen-Macaulay?

In particular, we will discuss the theory of Cohen-Macaulay rings, but will focus on techniques that show that all local rings are, in some sense, close to being Cohen-Macaulay.

Although we shall discuss the subject in much greater detail later, we give a brief discussion of Cohen-Macaulay rings here so that we can explain the sort of theorem we want to prove.

Recall the a ring R is *quasilocal* if it has a unique maximal ideal m: in this case we usually denote the residue class field R/m by K, and refer to the quasilocal ring $(R,\, m,\, K)$. We reserve the term *local ring* for a Noetherian quasilocal ring.

Let $(R,\, m,\, K)$ be a local ring of Krull dimension d. This implies that there exist d elements $x_1,\, \ldots\,, x_d \in m$ such that if $I = (x_1,\, \ldots\,, x_d)R$, then $\mathrm{Rad}\,(I) = m$. (One cannot use fewer than d elements, by the Krull height theorem.) Such a sequence of elements $x_1,\, \ldots\,, x_d$ is called a *system of parameters*. A d-tuple $(r_1,\, \ldots\,, r_d)$ is called a *relation* on $x_1,\, \ldots\,, x_d$ if

$$\sum_{j=1}^{d} r_j x_j = 0.$$

The relations are easily seen to be an R-submodule of the free R-module R^d. There are some obvious relations: the element

$$(0,\, \ldots\,,\, 0,\, x_j,\, 0,\, \ldots\,,\, -x_i,\, 0,\, \ldots\,,\, 0)$$

where x_j occurs in the i th spot and $-x_i$ occurs in the j th spot, is a relation. The elements in the R-span of these $\binom{d}{2}$ relations are referred to as *trivial relations*.

A local ring is called *Cohen-Macaulay* if there is a system of parameters such that every relation on the parameters is trivial. It then follows by a theorem that this is true for *every* system of parameters. By a theorem, this property passes to localizations. One then defines an arbitrary Noetherian ring to be *Cohen-Macaulay* if all of its localizations at maximal ideals (equivalently, at prime ideals) are Cohen-Macaulay.

In certain graded cases one can give an alternative characterization as follows. Let K be a field and R an $\mathbb{N}$-graded algebra (i.e., R has a direct sum decomposition $R = \bigoplus_{n=0}^{\infty} R_n$ with $1 \in R_0$ satisfying $R_m R_n \subseteq R_{m+n}$ for all $m, n \in \mathbb{N}$) such that R is finitely generated over $R_0 = K$. In this case, it turns out that one can always choose forms $F_1, \dots, F_d$ of positive degree in R (by raising the F_j to various powers one can even arrange that they all have the same degree) such that $F_1, \dots, F_d$ are algebraically independent over K and R is module-finite over $A = K[F_1, \dots, F_d]$. Of course, A is isomorphic with a polynomial ring in d variables over K. In this situation, R is Cohen-Macaulay if and only if R is free as an A-module.

In higher dimension, it is rare for modules over polynomial rings to be free. In fact, relatively few rings are Cohen-Macaulay. In equal characteristic 0, one can start taking module-finite extensions of a polynomial ring: if the dimension is 3 or higher, all sufficiently large such extensions fail to be Cohen-Macaulay.

Examples. Let $S = K[x, y]$ be the polynomial ring in two variables over the field K. Let $R = K[x^2, xy, y^2] \subseteq S$. One may take $A = K[x^2, y^2] \subseteq R$. Then R is free over A on the basis 1, xy, and so is Cohen-Macaulay.

On the other hand, let $R_1 = K[x^2, x^3, xy, y] \subseteq S$ and let $A_1 = K[x^2, y] \subseteq R_1$. Then R_1 is module-finite over A_1 with minimal generators 1, x^3, xy, but is *not* free over A_1. One has that $y(x^3) - x^2(xy) = 0$. This relation on minimal generators shows that R_1 is *not* A_1-free and therefore *not* Cohen-Macaulay. Alternatively, in the local ring of R_1 at its homogeneous maximal ideal, x^2, y is a system of parameters and $(xy, -x^3)$ is a non-trivial relation on x^2, y.

However, many of the rings that arise in natural geometric situations, such as complete intersections and rings defined by the vanishing of minors of a matrix of indeterminates *are* Cohen-Macaulay.

Many problems become easier in Cohen-Macaulay rings. One of the results we are aiming to prove, stated in a very special case, helps to remedy the situation when the ring is not Cohen-Macaulay:

Theorem. *Let R be a complete local domain of prime characteristic $p > 0$. Let $x_1, \dots, x_d$ be a system of parameters for R, and let $(r_1, \dots, r_d)$ be a relation on $x_1, \dots, x_d$. Then there is a complete local module-finite extension domain S of R such that the relation $(r_1, \dots, r_d)$ becomes trivial over S.*

This result has been known for well over a decade: cf. [M. Hochster and C. Huneke, *Infinite integral extensions and big Cohen-Macaulay algebras*, Annals of Math. **135** (1992), 53–89]. Recently there have been improvements: one can make all relations on all systems of parameters become trivial after just one module-finite extension (but new relations may be introduced). Beyond that, very recently, global versions of this theorem have been proved. We shall discuss the situation in detail later in the course.

The Theorem above turns out to be false when R contains a field of characteristic 0. Nonetheless, one can use the characteristic p results to prove important theorems in equal characteristic 0.

We next want to begin our systematic treatment of the theory of Gröbner bases. Before doing so we shall review some facts about closed algebraic sets in K^n over an algebraically closed field K.

Review of the behavior of closed algebraic sets over an algebraically closed field

This section is meant as an overview of some basic results on closed algebraic sets over an algebraically closed field. We give definitions and statements of some theorems, but most proofs are omitted. For a detailed treatment of this material, the reader may consult [R. Hartshorne, *Algebraic Geometry*, Springer-Verlag Graduate Texts in Mathematics **52**, New York • Berlin • Heidelberg, 1977], Chapter I. There is also a complete discussion in the Lecture Notes from Math 614, Fall 2003: see particularly the Lectures of October 3, 15, 17, and 20.

Let K be an algebraically closed field, and let $R = K[x_1, \, \dots \, , x_n]$ be a polynomial ring. If $W \subseteq R$ is any set,

$$\mathcal{V}(W) = \{v \in K^n : f(v) = 0 \text{ for all } f \in W\}.$$

It is easy to see that if I is the ideal generated by W, $\mathcal{V}(I) = \mathcal{V}(W)$. Moreover, if $f \in \mathrm{Rad}\,(I)$, i.e., $f^k \in I$ for some integer $k \geq 1$, then f also must vanish on $\mathcal{V}(I)$, and so $\mathcal{V}\big(\mathrm{Rad}\,(I)\big) = \mathcal{V}(W)$ as well. If $X = \mathcal{V}(I)$ for some ideal I, we say the X is a *closed algebraic set* in K^n, or a *Zariski* closed set in K^n. In fact, we have

(1) $K^n = \mathcal{V}(0)$ and $\emptyset = \mathcal{V}(R)$ are closed algebraic sets.

(2) $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$ for any two ideals I and J.

(3) $\mathcal{V}(\sum_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} \mathcal{V}(I_\lambda)$ for any family of ideals $\{I_\lambda\}_{\lambda \in \Lambda}$.

The conditions above show that the closed algebraic sets are, in fact, the closed sets of a topology on K^n: this is called the *Zariski topology.*

Suppose that we are given an arbitrary set of points $\mathcal{P} \subseteq K^n$ and we want to understand the Zariski closure $\overline{\mathcal{P}}$ of $\mathcal{P}$. Since this will be the smallest closed set containinng $\mathcal{P}$, we want to find I as *large* as possible such that $V(I) \supseteq \mathcal{P}$. But any element of I must vanish on $V(I)$, which we want to contain $\mathcal{P}$. Therefore, the largest ideal we can use is the ideal of *all* functions in $K[x_1, \, \dots \, , x_n]$ that vanish on $\mathcal{P}$, and this ideal defines $\overline{\mathcal{P}}$.

Note that if $n = 1$, the closed sets in K are the finite sets and K itself. In K^2 one gets finite unions of points and/or curves defined by one equation, and K^2 itself.

Every closed algebraic set $X \subseteq K^n$ inherits a Zariski topology, whose closed sets are simply the closed algebraic sets in K^n that happen to be contained in X.

The fundamental result in this area is:

Hilbert's Nullstellensatz. *Let K be an algebraically closed field and $R = K[x_1, \ldots, x_n]$ a polynomial ring over K. There is a bijective, order-reversing correspondence between closed algebraic sets in K^n and radical ideals of $K[x_1, \ldots, x_n]$. Under this correspondence, the radical ideal J corresponds to $\mathcal{V}(J)$, and the algebraic set X corresponds to the ideal $\mathcal{I}(X) = \{f \in R : \text{for all } v \in X,\, f(v) = 0\}$. In particular, the maximal ideals of R are in bijective correspondence with the points of K^n: given a point $v = (c_1, \ldots, c_n) \in K^n$, the corresponding maximal ideal consists of all polynomials that vanish at v. (It can also be described in terms of generators as the maximal ideal $(x_1 - c_1, \ldots, x_n - c_n)R$.)*

It follows that polynomials in $K[x_1, \ldots, x_n]$ have a common vanishing point if and only if they do not generate the unit ideal, and that $f \in \mathrm{Rad}\,(f_1, \ldots, f_m)$ if and only if f vanishes on $\mathcal{V}(f_1, \ldots, f_m)$. (Each of these statements is sometimes referred to as "Hilbert's Nullstellensatz.")

When $X = \mathcal{V}(I)$ we shall say that I is a *defining ideal* for X. When, in addition, I is radical we shall sometimes say that I is *the* defining ideal of X: it is now uniquely determined by X.

We want to make the closed algebraic sets over K into a category. When we want to emphasize that K^n is being thought of as an algebraic set, we use the notation $\mathbb{A}^n_K$ for K^n. Given closed algebraic sets $X \subseteq \mathbb{A}^m_K$ and $Y \subseteq \mathbb{A}^n_K$, we define a *$K$-regular* map or *$K$-morphism* from X to Y to be a function $\theta : X \to Y$ that is the restriction of a map $\mathbb{A}^m_K \to \mathbb{A}^n_K$ that is given in terms of coordinates by polynomials. That is, there are n polynomials $f_1, \ldots, f_n \in K[x_1, \ldots, x_m]$ such that for every point $v \in X$, $\theta(v) = \bigl(f_1(v), \ldots, f_n(v)\bigr)$.

Note that every K-regular map from X to Y is the restriction (where we restrict both the domain and the target) of a K-regular map $\mathbb{A}^m_K \to \mathbb{A}^n_K$. This may seem at first to be an unreasonably strong requirement, but one should keep in mind that given closed sets $X \subseteq \mathbb{R}^m$ and $Y \subseteq \mathbb{R}^n$, every continuous function from X to Y is the restriction of a continuous function from $\mathbb{R}^m \to \mathbb{R}^n$. To see this, one must show that the composition $X \to Y \subseteq \mathbb{R}^n$ extends to a map on $\mathbb{R}^m$. The composition is given in coordinates by n continuous maps $X \to \mathbb{R}$, and each of these can be extended to $\mathbb{R}^m$ by the Tietze extension theorem.

The identity map $X \to X$ is K-regular, and the composition of two K-regular maps is K-regular, so that the closed algebraic sets and K-regular maps form a category.

Given a closed algebraic set $X \subseteq \mathbb{A}^n_K$, the K-regular maps from X to $\mathbb{A}^1_K = K$ are simply the maps $X \to K$ arising from the restriction of a polynomial $f \in K[x_1, \ldots, x_n]$ to X. This set of maps forms a K-algebra, denoted $K[X]$, and called the *coordinate ring* of X. We have a surjection $K[x_1, \ldots, x_n] \twoheadrightarrow K[X]$ induced by restriction. The kernel is precisely the set of polynomials that vanish on X, or $\mathcal{I}(X)$, and so

$$K[X] \cong K[x_1, \ldots, x_n]/\mathcal{I}(X)$$

as K-algebras.

Recall that a ring is called *reduced* if every nilpotent element is 0. Then $K[X]$ is a reduced, finitely generated K-algebra. What is more, every reduced, finitely generated K-algebra occurs, up to K-algebra isomorphism, as $K[X]$ for some closed algebraic set X. For given such a K-algebra R, we may map $K[x_1, \ldots, x_n] \twoheadrightarrow R$ by choosing a finite set of, say, n generators for R as a K-algebra and sending the the x_j to these generators. The kernel is a radical ideal J. By Hilbert's Nullstellensatz, $J = \mathcal{I}(X)$ for a unique closed algebraic set X in $\mathbb{A}^n_K$. But then

$$R \cong K[x_1, \ldots, x_n]/J = K[x_1, \ldots, x_n]/\mathcal{I}(X) \cong K[X].$$

The map $X \mapsto K[X]$ is a contravariant functor from closed algebraic sets to reduced finitely generated K-algebras. Given a K-regular map $X \to Y$, one obtains a K-algebra homomorphism $K[Y] \to K[X]$ in an obvious way by composition: an element of $K[Y]$ is precisely a K-regular map $Y \to \mathbb{A}^1_K$, and the composite map $X \to Y \to \mathbb{A}^1_K$ is an element of $K[X]$.

The key result about this is:

Theorem. *Let K be an algebraically closed field. The category of closed algebraic sets over K and K-regular maps is anti-equivalent to the category of reduced, finitely generated K-algebras. The functor $X \mapsto K[X]$ provides the anti-equivalece.*

We shall not give a complete argument here, but we do indicate how one gets a contravariant functor from finitely generated reduced K-algebras to closed algebraic sets over K. The main point is that given a finitely generated reduced K-algebra R, one can give the set X of K-homomorphisms $R \twoheadrightarrow K$, which is in bijective correspondence with the set of maximal ideals of R, the "structure" of a closed algebraic set, i.e., one can put this set in bijective correspondence with the points of a closed algebraic set. Choices are made in setting up this correspondence, but the different closed algebraic sets obtained are canonically isomorphic in the category of closed algebraic sets.

Specifically, one simply maps a polynomial ring $K[x_1, \ldots, x_n] \twoheadrightarrow R$. Suppose that $R \cong K[x_1, \ldots, x_n]/J$, where J will be radical. Each K-algebra homorphism $R \twoheadrightarrow K$ gives a composite homomorphism $K[x_1, \ldots, x_n] \twoheadrightarrow R \twoheadrightarrow K$, and this map corresponds to a maximal ideal of $K[x_1, \ldots, x_n]$ and, hence, to a point of $\mathbb{A}^n_K$. The points obtained are precisely the points of $\mathcal{V}(J)$, which is therefore a closed algebraic set in bijective correspondence with $X = \mathrm{Hom}_{K-\mathrm{alg}}(R, K)$.

Some motivations for introducing Gröbner bases

Gröbner bases are a tool for doing explicit algorithmic calculations in a polynomial ring over a field K (or in a homomorphic image of a polynomial ring over K). Whether Gröbner basis methods actually give an algorithm depends on whether one can perform operations in K algorithmically. We shall not worry about this point. We simply assume that arithmetic operations in K are understood, and seek methods to solve problems in polynomial rings under the presumption that simple manipulations over the field can handled.

In dealing with Gröbner basis questions, unless otherwsie specified, K is always understood to be a field, and a given ring $K[x_1, \ldots, x_n]$ is meant to be assumed to be a polynomial ring in variables $x_1, \ldots, x_n$ over K.

We want to mention right away that while Gröbner bases are tools for calculation, they can also be used to prove substantial theorems, such as the Hilbert basis theorem (ideals in R are finitely generatded) and the Hilbert syzygy theorem (which is discussed further below). There are also many instances in which Gröbner basis techniques have been used to prove that certain infinite classes of rings of a special form have good properties.

Moreover, not surprisingly, the systematic study of Gröbner bases introduces a great many new theoretical problems.

Among the questions we want to consider are the following.

(1) Given generators $f_1, \ldots, f_m$ for an ideal of the polynomial ring $R = K[x_1, \ldots, x_n]$, how do we tell whether a given element $f \in R$ of the polynomial ring is in the ideal?

This is equivalent to determining whether one can solve the equation

$$f = U_1 f_1 + \cdots + U_m f_m$$

where the U_j are unknown elements of R.

If one knows an *a priori* bound D for the degrees of the unknown polynomials U_j in terms of m, n, and the degrees of the f_j, one can think of the U_j as polynomials of degree at most D with unknown coefficients. By working with coefficients, one gets a system of linear equations over K in the unknown coefficients, and the problem becomes pure linear algebra. The trouble with this idea is that while bounds for D are known, they are double exponential, making the implementation of this idea unfeasible. The complexity of the problem is double exponential in theory in worst cases, but the method of Gröbner bases often works in cases that arise in practice.

A similar problem arises in determining whether a given element is in the R-span of finitely many specified elements in the free module R^s. We shall give a Gröbner basis method that can be used for both of these problems.

(2) If we have finitely many generators for an ideal

$$I \subseteq K[x_1, \ldots, x_n] = R,$$

and $1 \le s \le n-1$, how can we find finitely many generators for $I \cap K[x_{s+1}, \ldots, x_n]$?

Here, we might intersect with the polynomial subring generated by an arbitrary subset of the variables, but by renumbering the indeterminates we might as well assume that the generators of the subring are $x_{s+1}, \ldots, x_n$. This type of question is part of what is called *elimination theory*: we are eliminating the variables $x_1, \ldots, x_s$ from the equations.

This sort of problem is intimately connected with the problem of solving explicitly the equations obtained by setting the generators of the ideal equal to 0.

To make this connection, we discuss the situation where K is algebraically closed.

We first want to understand the geometric meaning of the intersection of the ideal with the subring.

Proposition. *Let K be algebraically closed and let $I \subseteq K[x_1, \ldots, x_n]$ be any ideal. Suppose that $1 \le s \le n-1$ and let $J = I \cap K[x_{s+1}, \ldots, x_n]$. Let $\pi : \mathbb{A}^n_K \to \mathbb{A}^{n-s}_K$ be projection on the last $n-s$ coordinates. Let $X = \mathcal{V}(I) \subseteq \mathbb{A}^n_K$. Then $\mathcal{V}(J)$ is the Zariski closure of the projection $\pi(X)$.*

Proof. Let $f \in K[x_{s+1}, \ldots, x_n]$. By the discussion in the next to last paragraph on p. 3, f is in the defining ideal of Zariski closure of $\pi(X)$ if and only if f vanishes on $\pi(X)$, i.e., $f\big(\pi(X)\big) = 0$. This says that $f \circ \pi$, which is simply f thought of as a function on all of K^n (even though it only involves $x_{s+1}, \ldots, x_n$), vanishes on X, i.e., that $f \in I$. Thus, $I \cap K[x_{s+1}, \ldots, x_n]$ is a defining ideal for the Zariski closure of $\pi(X)$. □

Now suppose that $I = (f_1, \ldots, f_m) \subseteq K[x_1, \ldots, x_n]$. Note that the simultaneous solutions of the system

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

is the same as the set $V(I)$. Assume that $V(I)$ is a finite set. We next want to show if we have an algorithmic method for doing elimination theory, then we also have an algorithmic method for finding the solutions $V(I)$, *provided that we have a method for solving one polynomial equation in one variable over K.* The assumption that $V(I)$ is finite is not essential: if $V(I)$ is infinite, the method will show that.

The idea is very simple. One calculates $I \cap K[x_n]$. This is a principal ideal, since $K[x_n]$ is a PID. Thus, one gets a single generator $g(x_n) \in K[x_n]$ for the intersection. By the Proposition above, $gR[x_n]$ defines the Zariski closure of the projection of $V(I)$ on $\mathbb{A}^1_K = K$ corresponding to the last coordinate. There are three cases.

First case. The intersection is the (0) ideal. This implies that the Zariski closure of the projection is all of K, which means that the projection is an infinite set.

Second case. The intersection is the unit ideal, i.e., g is a nonzero constant. In this case, the projection is empty, and this means that there are no solutions.

Third case. g is a polynomial of positive degree. We are assuming that in this case we can find the roots of g in K: call them $\lambda_1, \ldots, \lambda_k$. This means that the closure of the projection of $V(I)$ is the set $\{\lambda_1, \ldots, \lambda_k\}$. This implies that the projection is finite, and since finite sets are closed, we must have that $\{\lambda_1, \ldots, \lambda_k\}$ *is* the projection. This means that the last coordinate of each point in $V(I)$ is one of $\lambda_1, \ldots, \lambda_k$, and that every λ_j occurs as the last coordinate of some point of $V(I)$. The problem of solving the original system of equations now breaks up into k separate problems, one for every λ_j. To find the points of $V(I)$ whose last coordinate is λ_j, substitute λ_j for x_n in each of the equations. This produces a new system of equations, but the number of variables is one smaller. Proceeding recursively, we eventually find all solutions of the original system.

(3) Another use of Gröbner bases is in solving the following kind of problem: given elements $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, find generators for all the relations on those elements, i.e., for the module of s-tuples of polynomials $(g_1, \ldots, g_s)$ such that $\sum_{j=1}^{m} g_j f_j = 0$. In fact, one can require insteasd that the g_i satisfy several equations like this, i.e., a system

$$\sum_{j=1}^{s} g_j f_{i,j} = 0, \quad 1 \le i \le r.$$

This is equivalent to finding the relations on the s columns of the $r \times s$ matrix $\mathcal{M} = \bigl(f_{i,j}\bigr)$, i.e., to finding the all the column vectors $\underline{g} = \begin{pmatrix} g_1 \\ \vdots \\ g_s \end{pmatrix}$ such that

$$\mathcal{M}\underline{g} = 0.$$

Consider the R-submodule M of R^s spanned by these columns. The module of relations on the columns is called a *first module of syzygies* of M. More generally, whenever we have a short exact sequence of finitely generated R-modules $0 \to M' \to R^k \to M \to 0$, M' is called a *first module of syzygies* of M. A first module of syzygies of a kth module of syzygies is called a $(k+1)$ *st module of syzygies*: when N is an nth module of syzygies of M there is an exact sequence

$$0 \to N \to R^{b_{n-1}} \to \cdots \to R^{b_0} \to M \to 0$$

of finitely generated R-modules.

Gröbner bases can be used to prove the famous Hilbert syzygy theorem, that every finitely generated module over $K[x_1, \ldots, x_n]$ has an nth module of syzygies that is free. (Equivalently, that every finitely generated R-module has a free resolution of length at most n.) Beyond that, Gröbner bases can be used to compute the resolution.

As a further application, Gröbner basis methods can be used in the graded case to calculate Hilbert functions. We shall discuss this in much greater detail, including a review of what is needed from the theory of Hilbert functions, once we have dome some basic Gröbner basis theory.